

ANONYMOUS ACQUISITION OF DIGITAL PRODUCTS BASED ON SECRET SPLITTING

ABSTRACT OF THE DISCLOSURE

5 An entity acquiring a digital product from a provider supplies acquisition-
related data such as an entity identification as well as information identifying a
provider of the product and, if applicable, a price of the product to an anonymity
service. In turn, the anonymity service splits each of these pieces of information into
a plurality of secret shares that are thereafter provided to corresponding sets of
10 shareholders. The anonymity service retains a transaction identification and identities
of the shareholders, but does not store or otherwise retain the secrets, i.e., the
acquisition-related data. When needed, the anonymity service reconstructs the secrets
by requesting the secret shares from the shareholders such that it can anonymously
fulfill the acquisition of the product. If later required, the anonymity service may
15 reconstruct the secrets for the purposes of auditing, legal investigations or the like. In
this manner, retraceable anonymous electronic transactions are made possible.

107E80 6E244550